添付資料

【今月の呼びかけ】

「 災害情報に便乗した罠（わな）に注意！ 」

東日本大震災により被災された皆さまに対し、心よりお見舞い申し上げます。

こうした災害に便乗し、被災者や被災地の復興支援者、災害情報に敏感になっている方々を騙（だま）そうとしたり、ウイルス感染させたりすることを目的とした罠メールが確認されています。パソコンの利用者は、こうした被害に遭わないためにもどのような手口の罠メールが存在するのかを理解し、少しでも不自然さを感じるメールはすぐに捨てるなど、慎重に対応するようにしてください。

（ご参考）
東北地方太平洋沖地震に便乗した悪さ（IPA 情報セキュリティブログ）
http://plaza.rakuten.co.jp/ipablog/diary/201103250000/

（1）罠メールの手口の概要

今回確認された罠メールの手口は、次の 3 つに分類されます。

表 1-1：罠メールの手口の分類と詳細

分類	詳細
デマ（混乱）	●チェーンメール これは、メールを「出来るだけ多くの人へ連鎖的に送る」ことを目的としており、内容に関係なく迷惑メール行為に当たります。内容によっては、受信者の不安感をいたずらに煽ることになり、その不安が連鎖的に広がることで風評被害を引き起こす原因にもなります。今回は、原発・放射線関連情報や節電の呼びかけ、寄付・募金や救援物資に関するメールが確認されています。 （ご参考） 東日本大震災　関連メール情報（迷惑メール相談センター） http://www.dekyo.or.jp/soudan/eq/
詐欺	●義援金詐欺メール これは、メール内に書かれているリンクをクリックさせて、被災者への義援金を騙し取る目的のウェブサイトに誘導する、いわゆるフィッシング詐欺の手口です。 （ご参考） 義援金詐欺等の悪質なメールにご注意ください！（総務省） http://www.soumu.go.jp/menu_kyotsuu/important/42233.html

ウイルス感染	●ウイルス感染を目的としたメール（ウイルスメール） 災害情報に見せかけた、ウイルスメールが確認されています。一見信頼できる情報のように見せかけるために、メール表題や添付ファイル名、本文がもっともらしい日本語になっていることがほとんどです。このメールの受信者は、このメールが信頼できるものと思い込み、添付ファイルを開くと、パソコンがウイルスに感染してしまいます。 以下に、IPA で確認しているウイルスメールの表題例を示します。 ➢ 被災者の皆様、とくにお子さんをお持ちの被災者の皆様へ ➢ 被ばくに対する防護対策について ➢ 全国へ計画停電のお知らせについて ➢ 福島原発最新状況 次に、IPA で確認しているウイルスメールの添付ファイル名の例を示します。 ➢ 放射線被ばくに関する基礎知識　第 1 報.doc、第 2 報.doc ➢ mSv（ミリシーベルト）で示した図解.doc ➢ 放射能が関東の人間に与える影響.doc ➢ 福島原発.doc ➢ 3 月 30 日放射線量の状況.doc 避難場所一覧表.xls ➢ 安定ヨウ素剤の服用量及び服用方法 （ご参考） IPA－災害情報を装った日本語のウイルスメールについて http://www.ipa.go.jp/security/topics/alert20110404.html

上述した手口の中でも、ウイルスメールには特に注意しなければなりません。次項では、今回実際に IPA で確認した罠メールについて説明します。

（2）ウイルスメールの詳細

（i）メール本文

メールが信頼できるものだと信じ込ませるための細工が、メール本文に施されています。図 1-1、図 1-2 は、今回確認されたウイルスメールの本文例です。

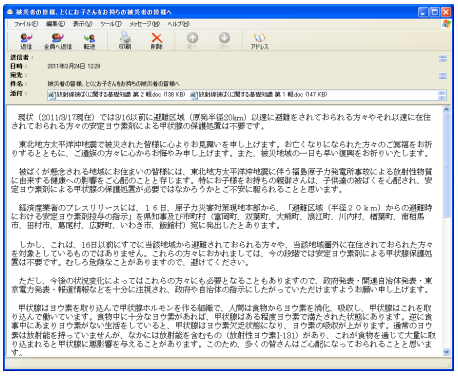

図 1-1：メール本文例 1

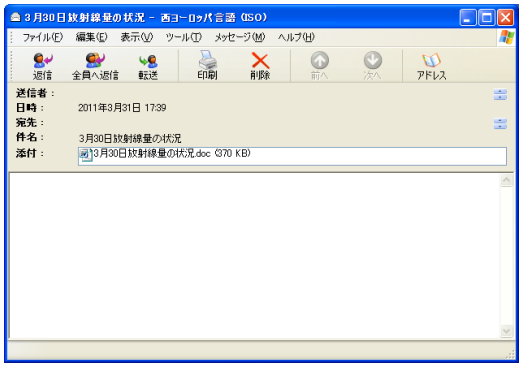

図 1-2：メール本文例 2

図 1-1 のメール本文には、このメールの送信者として詐称された組織の文書が、そっくりそのまま引用されています。こうすることで、当該組織からの本物のメールと思い込ませて添付ファイルを開かせます。

図 1-2 のメール本文には何も書かれていません。しかし、何も書かれていないことで添付ファイルの内容を確認したくなる心理を突いていると考えられます。

（ii）添付されているウイルス

ウイルスメールの添付ファイルを調べた結果、添付されていたウイルスは Mdropper と呼ばれるものでした。このウイルスは、日本マイクロソフト社のアプリケーションソフトである Word や Excel のドキュメントファイル内に、それらソフトの脆弱性（ぜいじゃくせい）を悪用する命令が仕込まれたものです。すなわち、ウイルスファイルのアイコンや拡張子は、Word や Excel そのものであるため、見た目ではウイルスかどうかの判断ができません（図 1-3 参照）。Mdropper は、さらに別のウイルスを呼び込む悪さをしますが、呼び込まれる別のウイルスが何なのかは感染時期によって異なり、どのような症状が出るかは一概には言えません。

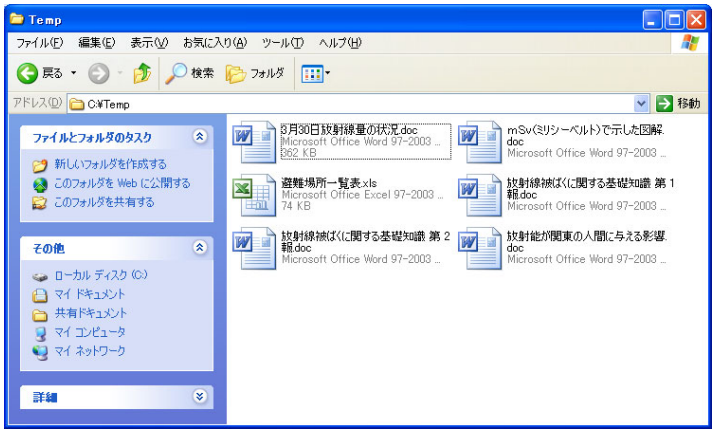

図 1-3：ウイルスメールの添付ファイル

悪用される脆弱性は次の 2 つです。

- Microsoft Office Word の脆弱性（MS10-087：CVE-2010-3333）
  http://www.microsoft.com/japan/technet/security/bulletin/ms10-087.mspx
- Microsoft Office Excel の脆弱性（MS09-067：CVE-2009-3129）
  http://www.microsoft.com/japan/technet/security/bulletin/ms09-067.mspx

（3）対策

（i）簡単にメールは開かない・クリックしない

普段やり取りがない送信者からのメールが届いたら、すぐに開いたり、中に書いてあるリンクをクリックしたりしないでください。可能であれば送信者と連絡を取り、本当にその送信者が送ったメールなのかを確認してください。ただし、確認をする際は、メールの中に書かれている連絡先には連絡をせず、出来る限り自分で連絡先を調べて電話で確認することを勧めます。

添付ファイルがあるメールであれば、普段やり取りのある送信者からのメールでも用心し、**少しでも不自然だと思うメールであれば、相手に確認を取るか、開かずに削除することが最善策です。**

（ii）脆弱性の解消

使用しているパソコンの、OS（オペレーティングシステム）やパソコンに導入しているアプリケーションソフトについては、できる限り最新版に更新し、脆弱性を解消してください。

（ご参考）

「Microsoft Update 利用の手順」（日本マイクロソフト社）

http://www.microsoft.com/japan/security/bulletins/j_musteps.mspx

「JVN iPedia 脆弱性対策情報データベース」（JVN）

http://jvndb.jvn.jp/

IPA では、ウイルスによって狙われることが多いアプリケーションソフトについて、それらがパソコンに導入されているか、および最新版となっているか否かをチェックできるツールを公開しています。詳しくは、下記の「MyJVN バージョンチェッカ」のウェブページを参照してください。

（ご参考）
「MyJVN バージョンチェッカ」（JVN）
http://jvndb.jvn.jp/apis/myjvn/#VCCHECK

（iii）ウイルス対策ソフトによる防御

ウイルス対策ソフトは万能ではありませんが、重要な対策の一つです。ウイルス対策ソフトを導入し、ウイルス定義ファイルを最新に保つことで、ウイルスの侵入阻止や、侵入したウイルスの駆除ができます。近年のウイルスは、パソコンの画面の見た目では感染していることが分からないものが多いため、ウイルスの発見と駆除には、ウイルス対策ソフトが必須です。

一般利用者向けのウイルス対策ソフトとしては、ウイルスの発見と駆除だけでなく、罠メールに書かれたリンクから危険なウェブサイトへ誘導された際にブロックを行う機能などを備える、「統合型」と呼ばれるものを推奨します。

（iv）復旧のための対策

パソコンの画面の見た目では感染していることが分からないが、怪しい添付ファイルを開いてしまったなどでパソコンの動作がおかしいと感じた場合は、お使いのウイルス対策ソフトで、ウイルス定義ファイルを最新の状態にしてからパソコン内のウイルスチェックを行ってください。

ウイルスを駆除できたとしても、パソコンが正常に動作していないと思われるのであれば、「システムの復元」を実施してください。これは、Windows XP、Vista、7 に搭載されている機能で、パソコンの情報を過去の状態に戻すことができます。なお、「システムの復元」を実施しても選択した日付から現在までに作成した文書や送受信したメール情報およびホームページへのアクセス履歴やお気に入りが消えることはありません。以下のマイクロソフトのサイトを参考にして、「システムの復元」を行ってください。

（ご参考）
「Windows XP 機能別紹介：システムの復元」（Windows XP）（日本マイクロソフト社）
http://www.microsoft.com/japan/windowsxp/pro/business/feature/performance/restore.mspx
「システムの復元とは」（Windows Vista）（日本マイクロソフト社）
http://windows.microsoft.com/ja-JP/windows-vista/What-is-System-Restore
「Windows 7 の機能：システムの復元」（Windows 7）（日本マイクロソフト社）
http://windows.microsoft.com/ja-JP/windows7/products/features/system-restore

なお、下記のウェブページにて、Windows を「セーフモード」で起動し、「システムの復元」を実施するための具体的な手順を案内しています。

（ご参考）
IPAー「Windows での「システムの復元」の実施手順」
http://www.ipa.go.jp/security/restore/

システムの復元が正常に完了しない場合は、パソコンを購入した時の状態に戻す作業（初期化）を行ってください。

実際の作業方法は、パソコンに付属の取扱説明書に記載されている「購入時の状態に戻す」などの手順に沿って作業してください。なお、作業を行う前には、重要なデータのバックアップを忘れずに行ってください。また、バックアップしたデータは、パソコンに戻す前にウイルス対策ソフトでウイルスチェックし、ウイルスが含まれていないことを確認してください。

（ご参考）
IPAーパソコンユーザのためのウイルス対策 7 箇条
http://www.ipa.go.jp/security/antivirus/7kajonew.html
IPAーパソコンユーザのためのスパイウェア対策 5 箇条
http://www.ipa.go.jp/security/antivirus/spyware5kajyou.html

（4）復旧・復興の支援活動をされている皆さまへ

今回の災害において復旧・復興支援活動をされている皆さまへのお願いです。

支援物資として送られる中古のパソコンは、最近は稼働していなかったものが多いと思われます。そのようなパソコンは、最近までの脆弱性が解消されていないため、ウェブページ閲覧やメールをする際にウイルス感染の被害に遭う可能性が高まります。被災地で稼働させる前に、OS やアプリケーションソフトを最新の状態に更新してください。

なお、Windows 98／Windows Me／Windows 2000 といった OS は日本マイクロソフト社によるサポートが既に終了しているため、脆弱性の解消を行うことができません。よって、インターネットに接続するだけで脆弱性を突かれてウイルス感染するなど、非常に危険な状態に陥る可能性が高くなります。これらの OS が入っているパソコンを被災地に送ることは、控えてください。